Η ΥΠΕΡΒΑΤΙΚΟΤΗΤΑ ΤΟΥ *e*

Για την απόδειξη της υπερβατικότητας του *e*, θα χρειασθούμε κάποιες βοηθητικές προτάσεις-λήμματα τις οποίες παραθέτουμε:

Λήμμα IV: • (i) Εάν p πρώτος και ν φυσικός με $(p,\nu)\neq 1$ (: δεν είναι πρώτοι προς αλλήλους), τότε $\nu = \text{πολ}\, p$.

- (ii) Εάν όμως $\nu \neq \text{πολ}\, p$ τότε $(p,\nu)=1$.
- (iii) Αν p πρώτος και $p/\alpha\cdot\beta$ τότε (p/α ή p/β)
- (iv) Αν ($p \nmid \alpha$ και $p \nmid \beta$) τότε $p \nmid \alpha\beta$
- (v) Αν ($p \nmid \alpha_1, p \nmid \alpha_2 ... p \nmid \alpha_\nu$) τότε $p \nmid \alpha_1\alpha_2...\alpha_\nu$
- (vi) Αν p πρώτος και ν φυσικός με $p>\nu$ τότε $p \nmid (\nu!)^p$
- (vii) Αν το p διαιρεί τους όρους ενός αθροίσματος πλην ενός, τότε δεν διαιρεί το άθροισμα.

Απόδειξη: (i) Έστω ότι $(p,\nu)=\delta>1$.

Τότε $\delta/p \Rightarrow$ (επειδή p πρώτος)

$(\delta = 1$ ή $p) \Rightarrow (\delta \neq 1)$

$$\delta = p \qquad (1)$$

Έτσι $\delta/\nu \underset{(1)}{\Rightarrow} p/\nu \Rightarrow \boxed{\nu = \text{πολ}\, p}$

(ii) Πρόκειται για την αντιθετοαντίστροφη πρόταση (i) άρα ισχύει.

(iii) Για την απόδειξη αυτή, θα χρησιμοποιήσουμε ένα θεμελιώδες θεώρημα της θεωρίας αριθμών που είναι το εξής: “Αν $(\alpha,\beta)=1$, τότε $\exists x \in$ Ù και $y \in$ Ù : $\alpha x + \beta y = 1$”.

Έτσι έχουμε:

Αν ($p/\alpha\beta$ και $p \nmid \alpha$) $\Rightarrow$ ($p/\alpha\beta$ και $\alpha \neq \text{πολ}\, p$)

$$\underset{\substack{\text{Λήμμα IV} \\ \text{(ii)}}}{\Rightarrow} (p/\alpha\beta \text{ και } (p,\alpha)=1) \qquad (2)$$

Όμως, από το θεμελιώδες θεώρημα της Θεωρίας Αριθμών, υπάρχει

$(x,y)\in \mathbb{Z}\times \mathbb{Z}: px+\alpha y=1$.

Έτσι η (2) γίνεται:

$$\left.\begin{cases} \alpha\beta = k\cdot p \\ px+ay=1 \end{cases}\right\} k\in \mathbb{Z} \qquad \begin{matrix}(3)\\(4)\end{matrix}$$

Επιλύομαι την (4) ως προς α και αντικαθιστούμε στην (3):

(Μπορούμε να υποθέσουμε ότι $y\neq 0$, διότι αν $y=0$, τότε $p=1$ και το συμπέρασμα καθίσταται προφανές, αφού $1/\beta$).

Έτσι: $$\frac{1-px}{y}\cdot\beta = kp \Rightarrow kyp=\beta(1-px)\Rightarrow$$

$$kyp=\beta-\beta px\Rightarrow (ky+\beta x)p=\beta\Rightarrow$$

$$\beta = \text{πολ}\, p\Rightarrow p/\beta .$$

Ομοίως δείχνουμε ότι αν $(p/\alpha\beta$ και $p\nmid\beta)$ τότε p/α.

Έτσι τελικά έχουμε την αποδεικτέα, δηλαδή

Αν $(p/\alpha\beta)$ τότε $(p/\alpha$ ή $p/\beta)$.

(iv) Πρόκειται για την αντιθετοαντίστροφη πρόταση (iii), άρα ισχύει.

(v) Η ισχύς της προτάσεως για $\nu=2$ απεδείχθη στο (iii).

Υποθέτουμε ότι: Αν $(p\nmid\alpha_1, p\nmid\alpha_2,\dots,p\nmid\alpha_k)$ τότε

$$p\nmid \alpha_1\cdot\alpha_2\dots\alpha_k \qquad (5)$$

Θα δείξουμε ότι: Αν $(p\nmid\alpha_1, p\nmid\alpha_2,\dots,p\nmid\alpha_k, p\nmid\alpha_{k+1})$ τότε

$$p\nmid \alpha_1\cdot\alpha_2\dots\alpha_k\cdot\alpha_{k+1} \qquad (6)$$

Από (5) έχομε $p\nmid\alpha_1\alpha_2\dots\alpha_k$ και από υπόθεση της (6) έχομε $p\nmid\alpha_{k+1}$.

Τότε από την ισχύ της πρότασης για $\nu=2$, έχομε ότι $p\nmid(\alpha_1\alpha_2\dots\alpha_k)\alpha_{k+1}$ δηλαδή $p\nmid\alpha_1\alpha_2\dots\alpha_k\alpha_{k+1}$, που είναι η αποδεικτέα.

(vi) Αν $p>\nu$, είναι προφανές ότι ο p δεν διαιρεί τον ν και οποιονδήποτε μικρότερό του . Δηλαδή

$$p\nmid\nu, p\nmid(\nu-1),\dots,p\nmid 2, p\nmid 1 \underset{(\mathrm{v})}{\Rightarrow} p\nmid\nu!$$

Επίσης

$$(\underbrace{p \nmid \nu!, p \nmid \nu!, ..., p \nmid \nu!}_{p \text{ επαναλήψεις}}) \underset{(\nu)}{\Rightarrow} p \nmid (\nu!)^p .$$

(vii) Αν $p \mid \alpha_1, p \mid \alpha_2 ... p \mid \alpha_k$ και $p \nmid a_{k+1}$, τότε αν θέσουμε

$$M = \alpha_1 + \alpha_2 + \alpha_3 + ... + \alpha_k + \alpha_{k+1} \Rightarrow$$

$$M = \pi_1 p + \pi_2 p + \pi_3 p + ... + \pi_k p + \alpha_{k+1} \Rightarrow$$

$$M = p(\pi_1 + \pi_2 + ... + \pi_k) + \alpha_{k+1} . \qquad (7)$$

Εάν τώρα υποθέσουμε ότι p / M, τότε $M = p\pi$ και η (7) δίνει

$$p\pi - p(\pi_1 + \pi_2 + ... + \pi_k) = \alpha_{k+1} \Rightarrow$$

$$p(\pi - \pi_1 - \pi_2 - ... - \pi_k) = \alpha_{k+1} \Rightarrow p / a_{k+1} \quad \text{άτοπο.}$$

Λήμμα V: Ισχύουν:

(i) $\lim\limits_{+\infty} x^n \cdot e^{-x} = 0, \quad n \in$ Í

(ii) $\int\limits_0^{+\infty} x^n e^{-x} dx = n!, \quad n \in$ Í $\qquad (1)$

Απόδειξη:

(i) $\lim\limits_{+\infty} x^n \cdot e^{-x} = \lim\limits_{+\infty} \frac{x^n}{e^x}$. Εφαρμόζουμε τον κανόνα του de' Hospital *n* φορές και έχομε:

$$\lim_{+\infty} \frac{x^n}{e^x} = \lim_{+\infty} \frac{(x^n)^{(n)}}{(e^x)^{(n)}} = \lim_{+\infty} \frac{n!}{e^x} = n! \lim_{+\infty} \frac{1}{e^x} \underset{e>1}{=} n! \frac{1}{\infty} = 0 .$$

(ii) Η απόδειξη θα γίνει με επαγωγή.

- Για $n = 0$ έχω

$$\int\limits_0^{+\infty} x^0 e^{-x} = \int\limits_0^{+\infty} e^{-x} = -\int\limits_0^{+\infty} (e^{-x})' = -[e^{-x}]_0^{+\infty} = -\lim_{+\infty} e^{-x} + e^{-0} = 0 + 1 = 1 = 0!$$

- Υποθέτουμε ότι η (1) ισχύει για $n = k$ δηλαδή

$$\int\limits_0^{+\infty} x^k \cdot e^{-x} = k! \qquad (2)$$

Θα δείξουμε ότι $\int\limits_0^{+\infty} x^{k+1} \cdot e^{-x} = (k+1)! \qquad (3)$

Πολλαπλασιάζουμε και τα δύο μέλη της (2) με $(k+1)$ και έχομε:

$$(k+1)\int_0^{+\infty} x^k e^{-x} = (k+1)\cdot k! \Rightarrow$$

$$\int_0^{+\infty} (k+1)x^k e^{-x} = (k+1)! \Rightarrow$$

$$\int_0^{+\infty} (x^{k+1})' e^{-x} = (k+1)! \Rightarrow$$

$$[x^{k+1}e^{-x}]_0^{+\infty} - \int_0^{+\infty} x^{k+1}(e^{-x})' = (k+1)! \Rightarrow$$

$$\lim_{+\infty} x^{k+1}e^{-x} - 0^{k+1}e^{-0} + \int_0^{+\infty} x^{k+1}e^{-x} = (k+1)! \Rightarrow \text{(i)}$$

$$0 - 0 + \int_0^{+\infty} x^{k+1}e^{-x} = (k+1)! \quad \text{που είναι η (3).}$$

Άρα $\int_0^{+\infty} x^n e^{-x} = n_0! \quad \forall\, n \in$ Í .

Θεώρημα: Ο e είναι υπερβατικός.

Απόδειξη: Έστω ότι ο e είναι αλγεβρικός. Τότε θα υπάρχει πολυώνυμο με ακεραίους συντελεστές του οποίου το e θα είναι ρίζα. Έστω $a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$, $a_0,\dots,a_n \in$ Ù με $a_n \neq 0$ το πολυώνυμο αυτό.

Ορίζουμε τους αριθμούς $M, M_1,\dots,M_n$ και $\varepsilon_1,\dots,\varepsilon_n$ ως εξής.

$$M = \int_0^{\infty} \frac{x^{p-1}[(x-1)\dots(x-n)]^p e^{-x}}{(p-1)!}dx$$

$$M_k = e^k \int_0^{\infty} \frac{x^{p-1}[(x-1)\dots(x-n)]^p e^{-x}}{(p-1)!}dx$$

$$e_k = e^k \int_0^{\infty} \frac{x^{-p}[(x-1)\dots(x-n)]^p e^{-x}}{(p-1)!}dx$$

Ο p παριστά ένα πρώτο αριθμό τον οποίο θα επιλέξουμε στη συνέχεια.

$$[(x-1)\dots(x-n)] = x^n + \dots \pm n! \Rightarrow$$

$$[(x-1)\dots(x-n)]^p = x^{np} + \dots + (n!)^p .$$

Έτσι το M γίνεται:

$$M = \int_0^{\infty} \frac{x^{p-1}(c_{np}x^{np} + ... + c_0)e^{-x}}{(p-1)!} dx$$

$$= \int_0^{\infty} \frac{(c_{np}x^{np+p-1} + ... + c_0 x^{p-1})e^{-x}}{(p-1)!}$$

$$= \frac{1}{(p-1)!}\int_0^{\infty} c_{np}x^{np+p-1}e^{-x}dx + ... + \frac{1}{(p-1)!}\int_0^{\infty} c_0 x^{p-1}e^{-x}dx$$

$$= \sum_{a=0}^{np} \frac{1}{(p-1)!} c_a \int_0^{\infty} x^{p-1+a}e^{-x}dx$$

όπου οι c_a είναι ακέραιοι και $c_0 = \pm(n!)^p$.

Αλλά από Λήμμα V(ii)

$$\int_0^{\infty} x^k e^{-x}dx = k!.$$

Άρα

$$M = \sum_{a=0}^{np} c_a \frac{(p-1+a)!}{(p-1)!}. \qquad (1)$$

Για $a = 0$ παίρνουμε τον όρο $c_0 \frac{(p-1+0)!}{(p-1)!} = \pm(n!)^p \frac{(p-1)!}{(p-1)} = \pm(n!)^p$.

Αν μάλιστα θεωρήσουμε $p > n$, τότε ο $(n!)^p$ δεν διαιρείται με το n, (Λήμμα IV vi) ενώ για κάθε $a > 0$ έχουμε τους όρους:

$$c_a \frac{(p-1+a)!}{(p-1)!} = c_a (p+a-1)(p+a-2)...p$$

που διαιρούνται όλοι με το p.

Άρα ο M, είναι ένας ακέραιος που γράφεται ως άθροισμα προσθετέων διαιρετών με το p, πλην ενός που δεν διαιρείται με το p.

Άρα (Λήμμα IV, (vii)) ούτε ο M διαιρείται με το p.

Θα εξετάσουμε τώρα τον M_k. Έχουμε:

$$M_k = e^k \int_k^{\infty} \frac{x^{p-1}[(x-1)...(x-n)]^p e^{-x}}{(p-1)!} dx$$

$$= \int_k^{\infty} \frac{x^{p-1}[(x-1)...(x-n)]^p e^{-(x-k)}}{(p-1)!} dx.$$

Θέτουμε $u = x - k \Rightarrow du = dx$

για $x = k \Rightarrow u = 0$

για $x \to +\infty \Rightarrow u \to +\infty$.

Άρα τα όρια ολοκλήρωσης αλλάζουν σε 0 και ∞ επομένως

$$M_k = \int_0^\infty \frac{(u+k)^{p-1}[(u+k-1)\ldots u \ldots (u+k-n)]^p e^{-u}}{(p-1)!} du .$$

Επειδή ο παράγοντας u μέσα στην αγκύλη βρίσκεται στην k-θέση και η p-δύναμη αυτής περιέχει τον παράγοντα u^p ολόκληρη η παράσταση

$$(u+k)^{p-1}[(u+k-1)\ldots u \ldots (u \pm k - n)]^p$$

είναι ένα πολυώνυμο με ακέραιους συντελεστές, του οποίου κάθε όρος έχει βαθμό τουλάχιστον p.

$$[(u+k-1)\ldots u \ldots (u+k-n)]^p = D'_{np} u^{np} + \ldots + D'_1 u^p$$

όπου $D'_{np} = 1$

$$(u+k)^{p-1} = u^{p-1} + \ldots + k^{p-1}$$

$$(u+k)^{p-1}[(u+k-1)\ldots u \ldots (u+k-n)]^p =$$

$$(u^{p-1} + \ldots + k^{p-1})(D'_{np}u^{np} + \ldots + D'_{np}u^{np} + \ldots + D'_1 u^p) =$$

$$D_{np} u^{(n+1)p-1} + \ldots + D_2 u^{p+1} + D_1 u^p$$

άρα

$$M_k = \int_0^\infty \frac{(D_{np}u^{(n+1)p-1} + \ldots + D_2 u^{p+1} + D_1 u^p)e^{-u}}{(p-1)!} du$$

$$= \int_0^\infty \frac{D_{np}u^{(n+1)p-1}}{(p-1)!} e^{-u} du + \ldots + \int_0^\infty \frac{D_1 u^p}{(p-1)!} e^{-u} du$$

$$= \frac{1}{(p-1)!} D_{np} \int_0^\infty u^{(n+1)p-1} e^{-u} du + \ldots + \frac{1}{(p-1)!} D_1 \int_0^\infty u^p e^{-u} du$$

$$= \sum_{a=1}^{np} \frac{1}{(p-1)!} D_a \int_0^\infty u^{p-1+a} e^{-u} du \overset{\text{Λήμμα V(ii)}}{=} \sum_{a=1}^{np} D_a \frac{(p-1+a)!}{(p-1)!}$$

όπου οι D_a είναι ακέραιοι.

Κάθε όρος του παραπάνω αθροίσματος διαιρείται με το p έτσι κάθε M_k είναι ένας ακέραιος που διαιρείται με p.

Επειδή το *e* υποθέσαμε ότι το *e* είναι ρίζα του πολυωνύμου

$a_n x^n + a_{n-1} x^{n-1} + ... + a_0 = 0$, τότε $a_n e^n + a_{n-1} e^{n-1} + ... + a_0 = 0, \ \ a_n \neq 0$.

Αντικαθιστώντας σ'αυτό τις σχέσεις

$$e^k = \frac{M_k + \varepsilon_k}{M} \quad k = 1,2,...,n$$

έχουμε

$$a_n \frac{M_n + \varepsilon_n}{M} + a_{n-1} \frac{M_{n-1} + \varepsilon_{n-1}}{M} + ... + a_0 = 0 \Rightarrow$$

$$a_n (M_n + \varepsilon_n) + a_{n-1} (M_{n-1} + \varepsilon_{n-1}) + ... + a_0 M = 0 \Rightarrow$$

$$(a_n M_n + ... + a_1 M + a_0 M) + (a_1 \varepsilon_1 + ... + a_n \varepsilon_n) = 0 \qquad (*)$$

Χωρίς να βλάπτεται η γενικότητα υποθέτουμε ότι $p > |a_0| \Rightarrow p \nmid a_0$.

Άρα ο *M* και ο a_0 δεν διαιρούνται με *p* κατά συνέπεια (Λήμμα IV (iv)) και ο $a_0 M$ δεν διαιρείται με *p*.

Αφού κάθε M_k διαιρείται με *p*, τότε ο αριθμός $a_1 M_1 + ... + a_n M_n$ διαιρείται με *p* και από Λήμμα IV(viii) ο αριθμός $a_0 M + a_1 M_1 + ... + a_n M_n$ δεν διαιρείται με *p*.

Ειδικότερα η επιλογή του *M* μπορεί να γίνει κατά τέτοιο τρόπο ώστε αναγκαστικά να είναι μη-αρνητικός ακέραιος.

Για να οδηγηθούμε σε αντίφαση και να δείξουμε ότι ο *e* είναι υπερβατικός αρκεί να δείξουμε ότι ο

$$|a_1 \varepsilon_1 + ... + a_n \varepsilon_n| \to 0 \qquad (1)$$

επιλέγοντας αρκετά μεγάλο *p*.

Για να δείξουμε την (1) αρκεί να δείξουμε ότι $|\varepsilon_k| \to 0 \ \ \forall \ k = 1,2,...,n$.

Επειδή *n* σταθερός αριθμός (βαθμός της πολυωνυμικής εξίσωσης), αν $1 \leq k \leq n$ τότε από

$$e^k = \frac{M_k + \varepsilon_k}{M} \Rightarrow \varepsilon_k = e^k M - M_k$$

$$\Rightarrow |\varepsilon_k| = |e^k M - M_k| \leq |e^k M| + |M_k| \leq |e^k M|$$

$$\Rightarrow |\varepsilon_k| \le e^k \int_0^k \frac{|x^{p-1}[(x-1)...(x-n)]^p|e^{-x}}{(p-1)!}dx$$

$$\le e^n \int_0^n \frac{n^{p-1}|[(x-1)...(x-n)^p|e^{-x}}{(p-1)!}dx$$

διότι από $0 \le x \le n \Rightarrow x^{p-1} \le n^{p-1}$.

Αν $A = \max|(x-1),...,(x-n)|$ για $x \in [0,n]$, τότε

$$|\varepsilon_k| \le e^n \int_0^n \frac{n^{p-1}A^p e^{-x}}{(p-1)!}dx \le \frac{e^n n^{p-1}A^p}{(p-1)!}\int_0^n e^{-x}dx \qquad (2)$$

και επειδή το ολοκλήρωμα $\int_0^n e^{-x}dx$

για $\quad -x = \omega \Rightarrow -dx = d\omega \Rightarrow dx = -d\omega$

για $\quad x = 0 \Rightarrow \omega = 0$

$x = n \Rightarrow \omega = -n$

δίνει ότι

$$\int_0^n e^{-x}dx = -\int_0^{-n} e^{\omega}d\omega = \int_{-n}^0 e^{\omega}d\omega = [e^{\omega}]_{-n}^0 = e^0 - e^{-n} = \frac{e^n - 1}{e^n} < 1. \qquad (3)$$

Έτσι η (2) λόγω (3) γίνεται:

$$|\varepsilon_k| \le \frac{e^n n^{p-1}A^p}{(p-1)!} \le \frac{e^n n^p A^p}{(p-1)!} = \frac{e^n (nA)^p}{(p-1)!}$$

και επειδή το $n \cdot A$ είναι σταθερά, τότε ο αριθμός $\frac{(nA)^p}{(p-1)!}$ μπορεί να γίνει μικρότερος από οποιονδήποτε $\varepsilon > 0$, αν πάρουμε το p αρκετά μεγάλο (Λήμμα II). Δηλαδή $|\varepsilon_k| < \varepsilon \ \forall \varepsilon > 0$. Έτσι $\varepsilon_k \to 0$ και ισχύει η (1).

Κατά συνέπεια, από (*) δεν μπορεί το άθροισμα δύο μη αρνητικών αριθμών να είναι μηδέν!

Η ΥΠΕΡΒΑΤΙΚΟΤΗΤΑ ΤΟΥ π

Ιστορία και σκιαγράφηση της απόδειξης: Η απόδειξη π που θα παρουσιασθεί, αφείλεται στον Lindemann και πραγματοποιήθηκε το 1882. Εκείνη η χρονιά θα μπορούσε να χαρακτηρισθεί ως το τέλος μιας υπερπροσπάθειας που είχε αρχίσει απ'τους Αρχαίους Έλληνες και αναφέρετο στον τετραγωνισμό του κύκλου με κανόνα και διαβήτη. Είναι γνωστό, ότι το πρόβλημα ανάγεται στην κατασκευή ευθύγραμμου τμήματος μήκους $\sqrt{\pi}$. Το γεγονός ότι ο π είναι αποδειχθεί ότι ήταν άρρητος, δεν απαγόρευε την κατασκευή του με κανόνα και διαβήτη, αφού και οι αριθμοί $\sqrt{2}$, $\sqrt{3}$ $\sqrt{5}$ κτλ. είναι άρρητοι μεν, αλλά κατασκευάσιμοι ευκόλως με την βοήθεια και του Πυθαγορείου Θεωρήματος. Η απόδειξη της υπερβατικότητας του π έθεσε τέρμα στις προσπάθειες τετραγωνισμού του κύκλου με κανόνα και διαβήτη, αφού μόνο αλγεβρικοί αριθμοί είναι κατασκευάσιμοι.

Η απόδειξη της υπερβατικότητας του π, έχει αξιοσημείωτες ομοιότητες με την απόδειξη της υπερβατικότητας του e!

Βεβαίως το προηγούμενο δεν είναι και τόσο παράξενο, αν σκεφθεί κάποιος ότι οι αριθμοί e και π δεν είναι τελείως άσχετοι, αλλά συνδέονται με μια εξαιρετικά απλή, όσο και όμορφη σχέση, γνωστότερη ως σχέση του Euler δηλ. $e^{i\pi} = -1$.

Την σχέση αυτή θα αποδείξουμε πριν την κύρια απόδειξη, αφού θα μας χρειασθεί ως λήμμα.

Επίσης θα μας χρειασθεί και η πρόταση ότι *"το γινόμενο δύο αλγεβρικών αριθμών είναι αλγεβρικός"*.

Η απόδειξη της παραπάνω βοηθητικής πρότασης, είναι αρκετά εκτεταμένη, αοφύ προϋποθέτει θεωρία των αλγεβρικών επεκτάσεων σωμάτων. Παρόλα ταύτα, δεν θα αφεθεί αναπόδεικτη. Όμως, η παρακολούθηση της απόδειξης, προϋποθέτει κάποιες στοιχειώδεις γνώσεις και ορισμούς, οι οποίες προϋποτίθενται. Αυτές είναι: Ορισμοί *δακτυλίου, σώματος και υποσώματος.*

Ορισμοί *διανυσματικού χώρου, υποχώρου, γραμμικώς ανεξάρτητα διανύσματα*

και γραμμικώς εξηρτημένα. Βάση και διάσταση διανυσματικού χώρου. Ακόμη για την απόδειξη της υπερβατικότητας του π θα χρειασθούν και κάποιες ιδιότητες των *συμμετρικών πολυωνύμων* όπως και των *στοιχειωδών συμμετρικών πολυωνύμων* τις οποίες θα αποδείξουμε.

Τέλος θα χρειασθούμε μια βοηθητική συνάρτηση την

$$F(x) = \frac{c^s}{(p-1)!} \cdot x^{p-1} \cdot (c_0 x^\tau + \ldots + c_\tau)^p$$

της οποίας μας ενδιαφέρουν οι παράγωγοι διαφόρου τάξεως (έως και p συγκεκριμένα).

Η διαδικασία αρχίζει με την απόδειξη του παρακάτω:

Λήμμα VI: Ισχύει η ισότητα $e^{i\pi} = -1$ (Euler)

Απόδειξη: Από σειρές Taylor για $z \in Â$ έχουμε:

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \ldots$$

$$\cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \ldots$$

$$e^z = 1 + \frac{z}{1!} + \frac{z^2}{2!} + \ldots \ .$$

Θέτουμε όπου z το iz:

$$e^{iz} = 1 + \frac{iz}{1!} + \frac{(iz)^2}{2!} + \frac{(iz)^3}{3!} + \frac{(iz)^4}{4!} + \frac{(iz)^5}{5!} + \ldots$$

$$= 1 + iz - \frac{z^2}{2!} - \frac{iz^3}{3!} + \frac{z^4}{4!} + \frac{iz^5}{5!} + \ldots$$

$$= \left(1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \ldots\right) + i\left(z - \frac{z^3}{3!} + \frac{z^5}{5!} - \ldots\right)$$

$$= \cos z + i \sin z \Rightarrow iz$$

$$e^{iz} = \text{συν} z + i\text{ημ} z \overset{z=\pi}{\Rightarrow} e^{i\pi} = \text{συν}\pi + i\text{ημ}\pi$$

$$\Rightarrow \boxed{e^{i\pi} = -1}$$

ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΑΛΓΕΒΡΙΚΩΝ ΕΠΕΚΤΑΣΕΩΝ

Ορισμός 1: Έστω F σώμα. Τότε ορίζουμε ως *δακτύλιο των πολυωνύμων της μεταβλητής* x:

$$F[x] = \{a_\nu x^\nu + ... + a_1 x + a_0 \,/\, a_i \in F,\ i = 0,1,2,...,\nu \ \text{ και } \ \nu = 0,1,2,...\}$$

Αν $a_\nu \neq 0$ τότε ορίζεται ως βαθμός του $f(x) = a_\nu x^\nu + ... + a_0$ ο αριθμός ν και γράφομε βαθμ$f(x) = \nu$ ή $\deg f(x) = \nu$. Ας σημειωθεί ότι το $F[x]$ δεν είναι σώμα, διότι π.χ. $x \in F[x]$ ενώ $x^{-1} \notin F[x]$.

Σημείωση: Για τις ανάγκες της απόδειξής μας για το π, αρκεί κάθε φορά να έχομε στο μυαλό μας ότι το σώμα F είναι το σύνολο των ρητών Ð. Παρόλα αυτά, θα δώσουμε στην συνέχεια γενικότερο ορισμό για το *αλγεβρικό στοιχείο επί σώματος*, όπως και της έννοιας *βαθμού αλγεβρικού στοιχείου*.

Οι γενικότεροι ορισμοί γενικεύουν και το θέμα, ενώ η θεώρηση του θέματος των πολυωνύμων με ακεραίους ή ρητούς συντελεστές μπορεί να αντιμετωπισθεί ισοδύναμα, *διότι κάθε πολυώνυμο με ρητούς συντελεστές, μπορεί με πολλαπλασιασμό με το ΕΚΠ των παρονομαστών να μετατραπεί σε πολυώνυμο ακεραίων συντελεστών ιδίου βαθμού, με ίδιες ρίζες* και να εξακολουθεί να είναι ανάγωγο, αν αρχικά ήταν ανάγωγο.

Ορισμός 2: (γενίκευση) Έστω F υπόσωμα του E και $a \in E$. αν υπάρχει πολυώνυμο $f(x) \in F[x]$, $f(x) \neq 0$ (: μηδενικού πολυωνύμου) με $f(a) = 0$, τότε λέμε ότι το α είναι *αλγεβρικό επί του F*. Αν δεν υπάρχει τέτοιο πολυώνυμο, λέμε ότι το α είναι *υπερβατικό επί του F.*

Παραδείγματα:

- Για $F =$ Ð, $E =$ Ñ, $\alpha = \sqrt{2}$ και $f(x) = x^2 - 2 \in$ Ð$[x]$ και $f[x] \neq$ μηδενικού πολ/σμού, έχω το συμπέρασμα ότι το $\sqrt{2}$ *είναι αλγεβρικό επί του* Ð.
- Επίσης για $F =$ Ð, $E =$ Â, $a = i$ και $f(x) = x^2 + 1 \in$ Ð$[x]$ και $f(x) \neq$ μηδενικού πολ/σμού, έχω το συμπέρασμα ότι i(: $\sqrt{-1}$) *είναι αλγεβρικός επί του* Ð.

Ορισμός 3: (γενίκευση) Αν $f(x0 \in F[x]$, $\deg f(x) \geq 1$, τότε το $f(x)$ θα λέγεται *ανάγωγο επί του F* αν για κάθε ανάλυση του $f(x)$ της μορφής $f(x) = f_1(x) \cdot f_2(x)$ με $f_1(x), f_2(x) \in F[x]$ να έπεται ότι $f_1(x)$ σταθερό πολυώνυμο ή $f_2(x)$ σταθερό πολυώνυμο.

Παραδείγματα:

- Τα x^2+1, $x+1$, x^3+2 είναι ανάγωγα επί του Ð.
- Τα x^2+1, $x+1$ είναι ανάγωγα επί του Ñ, όμως το x^3+2 δεν είναι ανάγωγο επί του Ñ, διότι $x^3+2 = (x+\sqrt[3]{2})(x^2-\sqrt[3]{2}-x+\sqrt[3]{4})$
- Το $x+1$ είναι ανάγωγο επί του Â, όμως το x^2+1 δεν είναι ανάγωγο επί του Â, διότι $x^2+1=(x+i)(x-i)$ και βεβαίως ούτε το x^3+2 είναι ανάγωγο επί του Â.

Ορισμός 4: (γενίκευση) Αν το *α* είναι ρίζα ενός αναγώγου πολυωνύμου $f(x) \in F[x]$ με $\deg f(x) = v$, τότε το *v* λέγεται *βαθμός* του αλγεβρικού στοιχείου *α*.

Παράδειγμα:

- Το *i* είναι ρίζα των πολυωνύμων x^2+1 και $x^4-1 \in$ Ð$[x]$ ο βαθμός όμως του *i* είναι 2, διότι το x^2+1 είναι ανάγωγο επί του Ð, ενώ το $x^4-1=(x^2-1)(x^2+1)$ δεν είναι ανάγωγο επί του Ð.

Ορισμός 5: Αν έχω έναν διανυσματικό χώρο *V* επί ενός σώματος *F*, τότε το πλήθος των στοιχείων μιας βάσης του V_F λέγεται *διάσταση* του V_F και συμβολίζεται με $\dim_F V$ ή $[V:F]$.

Παράδειγμα:

- $V = \{a_2x^2 + a_1x + a_0 / a_i \in$ Ñ$\}$. Τότε $V_{Ñ}$ είναι διανυσματικός χώρος και έχει ως βάση το $\{1, x, x^2\}$. Άρα $[v:$Ñ$]=3$.

Πρόταση 1: Αν *F* υπόσωμα του *E*, τότε το *E* είναι διαν. χώρος επί του *F*.

Ορισμός 6: Αν το F είναι υπόσωμα του E, τότε λέμε ότι το E είναι *επέκταση* του F και γράφουμε συμβολικά E/F.

Παραδείγματα:

- Το Ñ είναι επέκταση του Ð.
- Το Â είναι επέκταση του Ñ.

Ορισμός 7: Μια επέκταση E/F λέγεται *αλγεβρική* αν όλα τα στοιχεία του E είναι αλγεβρικά επί του F.

Ορισμός 8: Αν E/F και $[E:F]=v\in$ Ù$^{+}$, τότε η επέκταση E/F λέγεται *πεπερασμένη*.

Ορισμός 9: Έστω E/F και $a\in E$. Με $F(a)$ συμβολίζουμε την τομή όλων των υποσωμάτων του E που περιέχουν το F και το α. Δηλαδή το $F(a)$ είναι το ελάχιστο υποσώμα που περιέχει τα στοιχεία του F και το α.
Αποδεικνύεται ότι:

$$F(a)=\left\{\frac{f(a)}{g(a)}\Big/ f(x),g(x)\in F[x],g(a)\neq 0\right\}.$$

Γενικότερα αν $S\subseteq E$ με $F(S)$ συμβολίζουμε την τομή όλων των υποσωμάτων του E, που περιέχουν το F και το S.

Ορισμός 10: Ένα πολυώνυμο λέγεται *μονικός*, όταν ο συντελεστής του μεγιστοβαθμίου όρου του, είναι η μονάδα.

Ορισμός 11: Το πολυώνυμο $m(x)$ το οποίο είναι μονικό, μη μηδενικό και το ελαχίστου βαθμού που μηδενίζεται απ'το α καλείται *ελάχιστο πολυώνυμο* του α επί του F.

Αποδεικνύεται, ότι το ελάχιστο πολυώνυμο, είναι μονοσήμαντα ορισμένο.
Επίσης εξορισμού $F[a]=\{f(a)/f(x)\in F[x]\}$.

Πρόταση 2: Αν $f(x)$ το ελάχιστο πολυώνυμο του α επί του F, τότε το $f(x)$ ανάγωγο.

Απόδειξη: Αν $f(x) = g(x) \cdot h(x)$ με $g(x0, h(x) \in F[x]$ (1)

τότε $f(a) = 0$ και $g(a) \cdot h(x) = 0$ απ'όπου έχομε $g(a) = 0$ ή $h(a) = 0$.

Εάν τώρα κανένα απ'τα $g(x), h(x)$ δεν σταθερό πολυώνυμο, τότε απ'την (1) έχομε $\deg g(x) < \deg f(x)$ και $\deg h(x0 < f(x)$ πράγμα άτοπο, διότι το $f(x)$ είναι το πολυώνυμο ελαχίστου βαθμού με ρίζα το *α*.

Άρα ένα από τα δύο $g(x)$ και $h(x)$ πρέπει να είναι το σταθερό και έτσι το $f(x)$ είναι ανάγωγο.

Πρόταση 3: Αν το $f(x)$ είναι ανάγωγο επί του *F* με ρίζα $a \notin F$, τότε το $f(x)$ είναι το ελάχιστο πολυώνυμο του *α* επί του *F*.

Απόδειξη: Αν το $f(x)$ δεν ήταν το ελάχιστο πολυώνυμο του *α* επί του *F*, τότε θα υπήρχε ένα άλλο $g(x) \in F[x]$ με $\deg g(x) < \deg f(x)$ και $g(a) = 0$.

Έτσι,λόγω της προτάσεως 2, το $g(x)$ θα ήταν ανάγωγο επί του F.

Αυτό όμως είναι άτοπο διότι το ανάγωγο πολυώνυμο με ρίζα το *α* είναι μονοσήμαντα ορισμένο.

Πρόταση 4: Έστω E/F, $a \in E$ και *α* αλγεβρικό επί του *F*. Τότε ο διανυσματικός χώρος $F(a)$ επί του *F*, έχει ως βάση το σύνολο $\{1, a, a^2, ..., a^{v-1}\}$, όπου *ν* είναι ο βαθμός του αλγεβρικού στοιχείου *α*, επί του *F*.

Απόδειξη: Αν θεωρήσω το $m(x)$ ως ελάχιστο πολυώνυμο του *α* επί του *F*, τότε $\deg m(x) = V$. Επίσης τα διανύσματα $1, a, ..., a^{n-1}$ είναι γραμμικώς ανεξάρτητα επί του *F*.

Πράγματι· αν $b_0 + b_1 \cdot a + ... + b_{n-1}a^{n-1} = 0$ με $b_i \in F$, $i = 1,2,...,v-1$ τότε υποχρεωτικά $(b_0, b_1, ..., b_{v-1}) = (0,0,0,...,0)$ διότι διαφορετικά, το $g(x) = b_0 + b_1 x + ... + b_{v-1}x^{v-1}$ θα ήταν ένα μή μηδενικό πολυώνυμο, βαθμού μικρότερου του *ν* που θα είχε ρίζα το *α*, πράγμα άτοπο αφού ο βαθμός του *α* είναι *ν*.

Αν τώρα $\sigma(x) \in F[x]$ με $\deg \sigma(x) > v-1$, τότε $\exists\, q(x), \tau(x) \in F[x] : \sigma(x) =$

$q(x)\cdot m(x)+\tau(x)$ με $\tau(x)=0$ ή $\deg\tau(x)\leq \nu-1$.

Έτσι όμως επειδή $F[a]=F(a)$ έχω τα $\{1,a,...,a^{\nu-1}\}$ να παράγουν και τον χώρο $F(a)$, άρα η πρόταση απεδείχθη.

Πρόταση 5: Μια πεπερασμένη επέκταση είναι αλγεβρική επέκταση.

Απόδειξη: Έστω $[K:F]=n$. Έστω $a\neq 0,\ a\in K$ και οι δυνάμεις $a^0=1$, $a,a^z,...,a^n$. Τα $n+1$ αυτά στοιχεία είναι γραμμικά ανεξάρτητα επί του *F* γιατί $[K:F]=n$. Άρα υπάρχουν $c_0,c_1,c_2,...,c_n\in F$ με $(c_0,c_1,...,c_n)\neq(0,0,...,0)$ ώστε:

$$c_0+c_1\cdot a+c_2\cdot a^2+...+c_{n-1}\cdot a^{n-1}+c_n\cdot a^n=0 \qquad (1)$$

Ισχύει: $f(x)=c_0+c_1x+c_2x^2+...+c_{n-1}x^{n-1}+c_nx^n\in F[x]$ και είναι μη μηδενικό. Επίσης λόγω της (1) ισχύει $f(a)=0$. Άρα το *α* είναι αλγεβρικό επί του *F* και επειδή το *α* είναι τυχαίο στοιχείο του $K\Rightarrow$ κάθε στοιχείο του *K* είναι αλγεβρικό επί του *F*. Άρα η επέκταση K/F είναι αλγεβρική.

Πρόταση 6: Έστω *F*, *E*, *K* τρία σώματα με $F\subseteq E\subseteq K$. Αν οι E/F και K/E είναι πεπερασμένες επεκτάσεις, τότε και η K/F είναι πεπερασμένη επέκταση και $[K:F]=[K:E]\cdot[E:F]$

Απόδειξη: Έστω $A=\{a_1,a_2,...,a_n\}$ μια βάση του *K* επί του *E* και $B=\{\beta_1,\beta_2,...,\beta_n\}$ μια βάση του *E* επί του *F*. Θα αποδείξουμε ότι το σύνολο $M=\{a_i\beta_j\,/\,i=1,2,...,n,\ j=1,2,...,m\}$ είναι μια βάση του *K* επί του *F*.

Έστω $x\in K\Rightarrow x=c_1a_1+c_2a_2+...+c_na_n, c_i\in E$ αφού το σύνολο *A* είναι μια βάση του *K* επί του *E*.

Επίσης για κάθε c_i έχουμε $c_i=d_{i1}\beta_1+d_{i2}\beta_2+...+d_{im}\beta_m, d_{ij}\in F$, αφού το σύνολο *B* είναι μια βάση του *E* επί του *F*.

Άρα:

$$x=\sum_{i=1}^{n}c_ia_i=\sum_{i=1}^{n}\left(\sum_{j=1}^{m}d_{ij}\beta_j\right)a_i=\sum_{i=1,j=1}^{n,m}d_{ij}\beta_ja_i\ .$$

Άρα το M παράγει το K επί του F. Αρκεί να δείξουμε ότι τα στοιχεία του M είναι γραμμικά ανεξάρτητα.

Θεωρούμε ότι:

$$\sum_{i=1,j=1}^{n,m} d_{ij} a_i \beta_j = 0 \Rightarrow \sum_{i=1}^{n} \left(\sum_{j=1}^{m} d_{ij} \beta_j \right) a_i = 0 .$$

Επειδή το $\sum_{j=1}^{m} d_{ij} \beta_j \in E$ και το σύνολο A είναι βάση του K επί του E.

Παίρνουμε: $\sum_{j=1}^{m} d_{ij} \beta_j = 0,\ i = 1,2,...,n$.

Αλλά $d_{ij} \in F$ και το σύνολο B είναι βάση του E επί του F.

Άρα: $d_{ij} = 0,\ i = 1,2,...,n,\ j = 1,2,...,m$.

Επομένως το M είναι μια βάση του K επί του F. Επειδή $|M| = n \cdot m$ ισχύει:

$$[K : F] = [K : E] \cdot [E : F] .$$

Λήμμα VII: Αν α και β αλγεβρικοί αριθμοί επί του σώματος Å, τότε και το γινόμενό τους είναι αλγεβρικός αριθμός επί του σώματος Å.

Απόδειξη: Θεωρούμε την επέκταση Å(α, β). Έστω ότι ο α είναι αλγεβρικός n βαθμού και ο β m βαθμού. Τότε ισχύουν:

$$[Å(\alpha, \beta) : F(a)] = m \quad \text{και} \quad [Å((a) : Å] = n .$$

Αποδείξαμε (Πρόταση 6) ότι:

$$[Å(\alpha, \beta) : Å] = [Å(\alpha, \beta) : F(a)] \cdot [F(a) : F] = m \cdot n$$

και επειδή $m \cdot n$ πεπερασμένος αριθμός έπεται ότι η επέκταση $F(\alpha, \beta)/F$ είναι αλγεβρική.

Επειδή το Å(α, β) είναι σώμα, τότε θα είναι κλειστό ως προς την τάξη του πολλαπλασιασμού. Άρα επειδή $\alpha, \beta \in$ Å$(\alpha, \beta) \Rightarrow \alpha \cdot \beta \in$ Å(α, β).

Επομένως ο αριθμός $\alpha \cdot \beta$ είναι αλγεβρικός.

Ορισμός 12: Ένα πολυώνυμο $f(x_1, x_2, ..., x_n)$ μεταβλητές λέγεται συμμετρικό στις $x_1, x_2, ..., x_n$ αν παραμένει το ίδιο όταν εφαρμόσουμε μια μετάθεση στις μεταβλητές. Τα στοιχειώδη συμμετρικά πολυώνυμα είναι τα:

$$a_1 = \sum_{i=1}^{n} x_i$$

$$a_2 = \sum_{i<j} x_i x_j$$

$$a_3 = \sum_{i<j<k} x_i x_j x_k$$

$$\vdots$$

$$a_n = x_1 x_2 \cdots x_n,$$

δηλαδή το a_k είναι το άθροισμα όλων των γινομένων από k διαφορετικά μεταξύ τους από τα $x_1, x_2, ..., x_n$. Αποδεικνύεται ότι κάθε συμμετρικό πολυώνυμο είναι πολυώνυμο των στοιχειωδών συμμετρικών πολυωνύμων δηλαδή $f(x_1 x_2, ..., x_n) = g(a_1, a_2, ..., a_n)$ για κάποιο πολυώνυμο $\varphi(x_1, x_2, ..., x_n) \in \text{Đ}[x_1, x_2, ..., x_n]$.
(Βλέπε παρακάτω λήμμα VII(iii)).

Γενικά:
Αν $f(x)$ είναι ένα πολυώνυμο n βαθμού με διακριτές ρίζες $\rho_1, \rho_2, ..., \rho_n$ τότε:

$$\begin{aligned} f(x) &= a(x-\rho_1)(x-\rho_2)...(x-\rho_n) \\ &= a[x^n - (\rho_1 + \rho_2 + ... + \rho_n)x^{n-1} + (\rho_1\rho_2 + \rho_1\rho_3 + ... + \rho_{n-1} - \rho_n)x^{n-2} + ... \\ &\qquad + (-1)^n \rho_1\rho_2...\rho_n] \\ &= a[x^n - \mathrm{a}_1 x^{n-1} + \mathrm{a}_2 x^{n-2} - ... + (-1)^k \mathrm{a}_k x^{n-k} + ... + (-1)^n \mathrm{a}_n] \end{aligned}$$

όπου $a_k = \sum\limits_{i_1<i_2<...<i_k} \rho_{i_1}\rho_{i_2}...\rho_{i_k}$ είναι το k-οστό στοιχειώδες συμμετρικό πολυώνυμο στα $\rho_1, \rho_2, ..., \rho_n$.

Επομένως κάθε συμμετρικό πολυώνυμο των ριζών του $f(x)$ εκφράζεται ως πολυώνυμο των συντελεστών του πολυωνύμου $f(x)$.

Ορισμός 12: Έστω πολυώνυμο $f(x_1, x_2, ..., x_n)$ επί του σώματος *F*.

Έστω $ax_1^{\lambda_1} x_2^{\lambda_2} ... x_n^{\lambda_n}$, $\beta x_1^{\mu_1} x_2^{\mu_2} ... x_n^{\mu_n}$ δύο μονώνυμα. Υπάρχει ελάχιστος ακέραιος j τέτοιος ώστε $\lambda_j \neq \mu_j$. Λέμε ότι το $\beta x_1^{\mu_1} x_2^{\mu_2} ... x_n^{\mu_n}$ είναι μεγαλύτερο απ'το $ax_1^{\lambda_1} x_2^{\lambda_2} ... x_n^{\lambda_n}$ αν $\lambda_j > \mu_j$. Έτσι ορίζεται μια διάταξη στο σύνολο των

μονωνύμων. Ο μεγαλύτερο όρος (μονώνυμο) του $f(x_1,x_2,...,x_n)$ λέγεται *κύριο όρος* του πολυωνύμου.

Λήμμα VIII: Έστω ότι το πολυώνυμο $f(x_1,x_2,...,x_n)$ είναι συμμετρικό και ότι έχει κύριο όρο τον $ax_1^{u_1}x_2^{u_2}...x_n^{u_n}$. Τότε:

(i) $u_1 \geq u_2 \geq ... \geq u_n$

(ii) Το πολυώνυμο $\alpha \cdot \mathrm{a}_1^{u_1-u_2}\mathrm{a}_2^{u_2-u_3}...\mathrm{a}_{n-1}^{u_{n-1}}\mathrm{a}_n^{u_n}$ όπου $\mathrm{a}_1,\mathrm{a}_2,...,\mathrm{a}_n$ είναι τα στοιχειώδη συμμετρικά πολυώνυμα των $x_1,x_2,...,x_n$, έχει τον ίδιο κύριο όρο με το $f(x_1,x_2,...,x_n)$.

(iii) Το $f(x_1,x_2,...,x_n)$ μπορεί να γραφεί με την μορφή $g(\mathrm{a}_1,\mathrm{a}_2,...,\mathrm{a}_n)$ για κάποιο πολυώνυμο $g(x_1,x_2,...,x_n) \in F[x_1,x_2,...,x_n]$.

Απόδειξη:

(i) Το συμμετρικό πολυώνυμο $f(x_1,x_2,...,x_n)$ μαζί με τον κύριο όρο του $a \cdot x_1^{\kappa_1}x_2^{k_2}...x_i^{k_i}x_{i+1}^{k_{i+1}}...x_n^{k_n}$ πρέπει να έχει και τον όρο: $a \cdot x_1^{\kappa_1}x_2^{k_2}...x_i^{k_{i+1}}.x_{i+1}^{k_i}..x_n^{k_n}$. Απ'τον ορισμό του κύριου όρου παίρνουμε ότι $k_i \geq k_{i+1}$.

Άρα: $k_1 \geq k_2 \geq ... \geq k_n$.

(ii) Θέτουμε: $\sigma_i = k_i - k_{i+1}$, $i = 1,2,...,n-1$ και $\sigma_n = k_n$. Τότε ισχύει: $\sigma_i \geq 0$, $i = 1,2,...,n$. Ένας όρος του $a \cdot \mathrm{a}_1^{\sigma_1}\mathrm{a}_2^{\sigma_2}...\mathrm{a}_n^{\sigma_n}$ θα είναι της μορφής $a \cdot x_1^{\mu_1}x_2^{\mu_2}...x_n^{\mu_n}$, όπου κάθε μ_i είναι άθροισμα ορισμένων απ'τους $\sigma_1,\sigma_2,...,\sigma_\mu$. Επειδή ο κύριος όρος πρέπει να έχει το μεγαλύτερο δυνατό μ_1, ο εκθέτης του x_1 στον κύριο όρο είναι ο $\mu_1 = \sigma_1 + \sigma_2 + \sigma_{n-1} + ... + \sigma_n =$ $(k_1 - k_2) + (k_2 - k_3) + ... + (k_{n-1} - k_n) + k_n = k_1$.

Όμοια για το μέρος $x_2^{\mu_2} \cdot x_3^{\mu_3}...x_n^{\mu_n}$ του κύριου όρου κάνουμε τον ίδιο συλλογισμό και βρίσκουμε ότι ο εκθέτης είναι ο $\sigma_2 + \sigma_3 + ... + \sigma_n = k_n$ κ.λπ.

Άρα ο κύριος όρος του $a \cdot \mathrm{a}_1^{k_1-k_2}\mathrm{a}_2^{k_2-k_3}...\mathrm{a}_n^{k_n}$ είναι ο ίδιος με τον κύριο όρο του $f(x_1,x_2,...,x_n)$.

(iii) Θεωρούμε το πολυώνυμο

$$f_1(x_1,x_2,...,x_n) = f(x_1,x_2,...,x_n) - a \cdot \mathrm{a}_1^{k_1-k_2}...\mathrm{a}_n^{k_n}$$

Το $f_1(x_1,x_2,...,x_n)$ είναι συμμετρικό πολυώνυμο και έχει κύριο όρο μικρότερο από τον κύριο όρο του $f(x_1,x_2,...,x_n)$. Έστω $b \cdot x_1^{\lambda_1}x_2^{\lambda_2}...x_n^{\lambda_n}$ ο κύριος όρος του $f_1(x_1,x_2,...,x_n)$.

Θεωρούμε το πολυώνυμο:

$$f_2(x_1,x_2,...,x_n) = f_1(x_1,x_2,...,x_n) - a_1 \cdot \mathrm{a}_1^{\lambda_1-\lambda_2}...\mathrm{a}_n^{\lambda_n}$$

το οποίο έχει κύριο όρο μικρότερο του κύριου όρου του $f_1(x_1,x_2,...,x_n)$. Συνεχίζουμε με τον ίδιο τρόπο και επειδή υπάρχουν πεπερασμένα το πλήθος πολυώνυμα μικρότερα από τα $x_1^{k_1}x_2^{k_2}...x_n^{k_n}$ η παραπάνω διαδικασία θα τελειώσει μετά από πεπερασμένο το πλήθος βήματα έστω m και το $f_m(x_1,x_2,...,x_n)$ θα είναι ένα σταθερό πολυώνυμο $c \in F$.

Άρα $f(x_1,x_2,...,x_n) = a \cdot \mathrm{a}_1^{k_1-k_2}...\mathrm{a}_n^{k_n} + a_1 \cdot \mathrm{a}_1^{\lambda_1-\lambda_2}...\mathrm{a}_n^{\lambda_n} + ... + c$ και εάν

$g(x_1,x_2,...,x_n) = a \cdot \mathrm{a}_1^{k_1-k_2}...\mathrm{a}_n^{k_n} + a_1 \cdot \mathrm{a}_1^{\lambda_1-\lambda_2}...\mathrm{a}_n^{\lambda_n} + ... + c \in F[x_1,x_2,...,x_n]$

τότε: $f(x_1,x_2,...,x_n) = g(\mathrm{a}_1,\mathrm{a}_2,...,\mathrm{a}_n)$.

Λήμμα IX: Για την συνάρτηση

$$F(x) = \frac{c^s}{(p-1)!} \cdot x^{p-1} \cdot (c_0 x^\tau + ... + c_\tau)^p$$

λαμβάνω τις παρακάτω μορφές για τις παραγώγους των διαφόρων τάξεων.

Έχουμε:

$$F(x) = \frac{c^s}{(p-1)!} x^{p-1}(c_0^p x^{rp} + ... + c_r^p) \Rightarrow$$

$$F(x) = \frac{c^s}{(p-1)!}\left(c_0^p x^{rp+p-1} + ... + c_r^p x^{p-1}\right)$$

Οπότε

$$F^{(1)}(x)=\frac{c^5}{(p-1)!}[c_0^p(rp+p-1)x^{rp+p-2}+...+c_r^p(p-1)x^{p-2}]$$

$$F^{(2)}(x)=\frac{c^s}{(p-1)!}[c_0^p(rp+p-1)(rp+p-2)x^{rp+p-3}+...+c_r^p(p-1)(p-2)x^{p-3}]$$

$$\vdots$$

$$F^{(p-2)}(x)=\frac{c^s}{(p-1)!}[c_0^p(rp+p-1)(rp+p-2)...(rp+p-p+2)x^{rp+p-1-p+2}$$

$$+...+c_r^p(p-1)(p-2)...2x]\Rightarrow$$

$$F^{(p-2)}(x)=\frac{c^s}{(p-1)!}[c_0^p(rp+p-1)(rp+p-2)...(rp+2)x^{rp+1}+...+c_r^p(p-1)!x]$$

$$F^{(p-1)}(x)=\frac{c^s}{(p-1)!}[c_0^p(rp+p-1)(rp+p-2)...(rp+2)(rp+1)x^{rp}+...+c_r^p(p-1)!]$$

$$F^{(p)}(x)=\frac{c^s}{(p-1)!}[c_0^p(rp+p-1)(rp+p-2)...(rp+2)(rp+1)rp\cdot x^{rp-1}+...+\pi!c_{r-1}^p+0]$$

Θεώρημα (Lindemann): Ο πραγματικός αριθμός π είναι υπερβατικός.

Απόδειξη: Θα το αποδείξουμε με τη μέθοδο της εις άτοπον απαγωγής.

Έστω ότι ο π είναι αλγεβρικός, τότε και το γινόμενο $i\pi$ (όπου $i=\sqrt{-2}$) είναι αλγεβρικός αριθμός (Λήμμα VII). Άρα ο αριθμός $i\pi$ είναι ρίζα ενός πολυωνύμου μή μηδενικού. Έστω ότι το πολυώνυμο αυτό είναι το $\Phi(x)$ με ρητούς συντελεστές και με ρίζες τους αριθμούς: $a_1=i\pi$, $a_2,a_3,...,a_n$. Είναι γνωστό (Λήμμα VI) ότι: $e^{i\pi}+1=0$. Επομένως:

$$(e^{a_1}+1)(e^{a_2}+1)...(e^{a_n}+1)=0 \qquad (1)$$

(Αφού $e^{a_1}+1=0$)

Κάνοντας τις πράξεις στο 1ο μέλος της ισότητας (1) βρίσκουμε ένα άθροισμα δυνάμεων με βάση το e και εκθέτες αθροίσματα της μορφής $a_{i_1}+a_{i_2}+...+a_{i_m}$.

Για παράδειγμα ο όρος $e^{a_j}e^{a_m}e^{a_{i-1}}e^{a_i}1\cdot 1...1=e^{a_j+a_m+a_{i-1}+a_i}$.

Υπάρχει ένα πολυώνυμο που έχει ως ρίζες, όλα τα αθροίσματα της μορφής: $a_{i_1}+a_{i_2}+...+a_{i_m}$, του οποίου οι συντελεστές, είναι συμμετρικά πολυώνυμα

των $a_1, a_2, ..., a_n$ και άρα πολυώνυμα των συν/τών του $\Phi(x)$, που είναι ρητοί αριθμοί.

Διαιρώντας το πολυώνυμο αυτό με το x^{n-r} (r το πλήθος των μη μηδενικών εκθετών της 1) και πολλαπλασιάζοντας με το ΕΚΠ των παρονομαστών του $\Phi(x)$ βρίσκουμε ένα πολυώνυμο $f(x)$ με ακέραιους συντελεστές και ρίζες τους μη μηδενικούς εκθέτες $\beta_1, \beta_2, ..., \beta_r$ στο ανάπτυγμα της (1).

Έτσι η (1) αναπτύσσεται:

$$e^{\beta_1} + e^{\beta_2} + ... + e^{\beta_r} + e^0 + e^0 + ... + e^0 = 0 \Rightarrow$$

$$e^{\beta_1} + e^{\beta_2} + ... + e^{\beta_r} + k = 0 \quad \text{όπου} \quad k \in Í\,. \qquad (2)$$

Στο ανάπτυγμα της (1) υπάρχει ο όρος $1 \cdot 1 ... 1$. Επομένως $\kappa > 0$. Έστω ότι:

$$f(x) = cx^r + c_1 x^{r-1} + ... + c_{r-1}x + c_r \quad \text{με} \quad c_r \neq 0$$

(διότι το 0 δεν είναι ρίζα του $f(x)$).

Ορίζουμε $F(x) = \dfrac{c^s x^{p-1}\{f(x)\}^p}{(p-1)!}$, όπου $s = r(p-1)$ με p πρώτο αριθμός. (3)

Επίσης ορίζουμε: $g(x) = F(x) + F'(x) + ... + F^{(s+p+r-1)}(x)$.

Ισχύει: $\deg F(x) = (p-1) + rp = p - 1 + rp$ και

$$s + p + r - 1 \overset{(3)}{=} r(p-1) + p + r - 1 = rp - \cancel{r} + p + \cancel{r} - 1 = rp + p - 1\,.$$

Άρα $F^{(s+p+r)}(x) = 0$. Επίσης $g'(x0 = F'(x) + F^{(2)}(x) + ... + F^{(s+p+r-1)}(x)$.

Υπολογίζουμε την:

$$\begin{aligned}\frac{d}{dx}[e^{-x}g(x)] &= -e^{-x}g(x) + e^{-x}g'(x) \\ &= -e^{-x}[g(x0 - g'(x)] \\ &= -e^{-x}[F(x) + F'(x) + ... + F^{(s+p+r-1)}(x) \\ &\qquad - F'(x) - F^{(2)}(x) - ... - F^{(s+p+r-1)}(x)] \\ &= -e^{-x}F(x)\,.\end{aligned}$$

Επομένως:

$$\int_0^x [e^{-t}g(t)]'dt = -\int_0^x e^{-y}F(y)dy \Rightarrow e^{-x}g(x) - e^{-0}g(0) = \int_0^x e^{-y}F(y)dy$$

$$\Rightarrow e^{-x}g(x)-g(0)=-\int_0^x e^{-y}F(y)dy.$$

Αν θέσουμε $y=\lambda\cdot x$ (προσοχή! η μεταβλητή είναι το λ) έχουμε για τα νέα όρια ολοκλήρωσης $\left\{\begin{matrix} y=0\rightarrow\lambda=0 \\ y=x\rightarrow\lambda=1\end{matrix}\right\}$ και

$$e^{-x}g(x)-g(0)=-\int_0^1 e^{-\lambda x}F(\lambda x)d(\lambda x)\Leftrightarrow$$

$$\Leftrightarrow e^{-x}g(x)-g(0)=-x\int_0^1 e^{-\lambda x}F(\lambda x)d\lambda \overset{(\text{πολ/ζω } \cdot e^x)}{\Leftrightarrow}$$

$$\Leftrightarrow e^x\cdot e^{-x}g(x)-e^x g(0)=-x\int_0^1 e^x\cdot e^{-\lambda x}F(\lambda x)d\lambda$$

$$\Leftrightarrow g(x0-e^x g(0)=-x\int_0^1 e^{(1-\lambda)x}F(\lambda x)d\lambda.$$

Αν θέσουμε στη θέση του x διαδοχικώς τα $\beta_1,\beta_2,...,\beta_r$, τότε παίρνουμε:

$$g(\beta_1)-e^{\beta_1}g(0)=-\beta_1\int_0^1 e^{(1-\lambda)\beta_1}F(\lambda\beta_1)d\lambda$$

$$g(\beta_2)-e^{\beta_2}g(0)=-\beta_2\int_0^1 e^{(1-\lambda)\beta_2}F(\lambda\beta_2)d\lambda$$

$$\vdots \qquad \vdots \quad \vdots \qquad \vdots \qquad \vdots$$

$$g(\beta_r)-e^{\beta_r}g(0)=-\beta_r\int_0^1 e^{(1-\lambda)\beta_r}F(\lambda\beta_r)d\lambda.$$

Προσθέτουμε κατά μέλη, χρησιμοποιώντας την ισοδύναμη σχέση της (2), ότι $-(e^{\beta_1}+e^{\beta_2}+...+e^{\beta_r})=k$ Έτσι βρίσκουμε:

$$\sum_{j=1}^r g(\beta_j)+k\cdot g(0)=-\sum_{j=1}^r \beta_r\int_0^1 e^{(1-\lambda)\beta_r}F(\lambda\beta_r)d\lambda \qquad (**)$$

Ισχυρισμός: Ισχύει ότι $\sum_{j=1}^r F^{(t)}(\beta_j)=0$, για $0<t<p$.

Πράγματι˙ Αν παραγωγίσουμε την $F(x)$ μέχρι και $p-1$ φορές, θα εμφανίζεται πάντα ο παράγοντας $f^{(m)}(x)$ με $1\le m\le p-1$.

Αλλά $f(\beta_i)=0$, για κάθε $i=1,2,...,r$. Άρα $f^{(m)}(\beta_i)=0$.

Άρα $\sum_{j=1}^r F^{(t)}(\beta_j)=0$, για $0<t<p$. ■

Αν $t \geq p$ η $F^{(t)}(x)$ δεν έχει παράγοντα της μορφής $f^{m}(x)$. Άρ $F^{(t)}(\beta_i) \neq 0$, $\forall\ t \geq p$. Επίσης το $F^{(t)}(x)$ έχει παράγοντα τον αριθμό p (βλέπε λήμμα VIII). Το ίδιο ισχύει για $t > p$.

Άρα για οποιοδήποτε $t \geq p$ το άθροισμα: $\sum_{j=1}^{r} f^{(t)}(\beta_j)$ είναι ένα συμμετρικό πολυώνυμο των β_j βαθμού $\leq rp-1$ δηλαδή βαθμού $\leq s$. Δηλαδή είναι ένα πολυώνυμο βαθμού $\leq s$ των συντελεστών $c_{i/c}$. Το c^{s} έχει τεθεί στον ορισμό της $f(x)$ για να κάνει αυτό το άθροισμα έναν ακέραιο.

Άρα για $p \geq s$ έχουμε:

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = p\lambda_t \qquad (*)$$

για κάποιο $\lambda_t \in$ Ù.

Άρα

$$\sum_{j=1}^{r} g(\beta_j) = \sum_{j=1}^{r} [F(\beta_j) + F'(\beta_j) + \ldots + F^{(s+p+r-1)}(\beta_j)]$$

$$= \sum_{j=1}^{r} F(\beta_j) + \sum_{j=1}^{r} F'(\beta_j) + \ldots + \sum_{j=1}^{r} (s+p+r-1)(\beta_j)$$

$$\overset{(*)}{=} p \cdot \lambda_0 + p \cdot \lambda_1 + \ldots + p \cdot \lambda_{s+p+r-1}$$

$$= p \cdot (\lambda_0 + \lambda_1 + \ldots + \lambda_{s+p+r-1}) = p \cdot \lambda, \quad \lambda \in \text{Ù}.$$

Τώρα θα ελέγξουμε το $g(o)$.

(i) Αν $t \leq p-2$ τότε $F^{(t)}(0) = 0$

(ii) Αν $t = p-1$ τότε $F^{(t)}(0) = c^{s} \cdot c_r^{p}$

(iii) Αν $t \geq p$ τότε $F^{(t)}(0) = p \cdot l_t$ για κατάλληλο $l_t \in$ Ù. Παράδειγμα για $t = p \Rightarrow l_p = c^{s} \cdot c_{r-1}^{p}$.

Τα ανωτέρω συμπεράσματα προκύπτουν από το λήμμα IX.

Επομένως: $g(0) = c^{s} \cdot c_r^{p} + l \cdot p$, για $l \in$ Ù. $(l = l_p + l_{p+1} + \ldots + l_{rp+p-1})$.

Άρα βρήκαμε ότι το 1ο μέλος της ισότητας (**) είναι

$$p \cdot \lambda + k \cdot (c^{s} \cdot c_r^{p} + lp) = p\lambda + k \cdot c^{s} \cdot c_r^{p} + klp =$$

$$= (\lambda + kl)p + k \cdot c^s \cdot c_r^p = z \cdot p + k \cdot c^s \cdot c_r^p, \quad z \in \mathbb{Z}.$$

Ισχύουν: $k \neq 0,\ c \neq 0, c_r \neq 0$. Άρα αν πάρουμε το $p > \max(k, |c|, |c_r|)$, τότε το πρώτο μέλος της σχέσης (**) είναι ένας ακέραιος που δεν διαιρείται από το p και επομένως είναι διάφορος από το μηδέν.

Για το δεύτερος μέλος της σχέσης (**) έχουμε:

$$|F(\lambda\beta_j)| \leq \left| \frac{c^s}{(p-1)!} \cdot (\lambda\beta_j)^{p-1} \cdot \{f(\lambda\beta)\}^p \right| = \left| \frac{c^s}{(p-1)!} \right| \cdot |\lambda|^{p-1} \cdot |\beta_j|^{p-1} \cdot |f(\lambda\beta_j)|^p$$

$$= \left| \frac{c^s}{(p-1)!\beta_j} \right| \cdot |\lambda|^{p-1} \cdot |\beta_j|^p \cdot |f(\lambda\beta_j)|^p$$

$$\leq \left| \frac{c^s}{(p-1)!\beta_j} \right| \cdot |\beta_j \cdot f(\lambda\beta_j)$$

$$\leq \frac{|c|^s \cdot \{m(j)\}^p}{|\beta_j| \cdot (p-1)!}$$

όπου $m(j) = |\beta_j| \cdot \sup\limits_{0 \leq \lambda \leq 1} |f(\lambda\beta_j)$.

Και:

$$\left| -\sum_{j=1}^{r} \beta_j \cdot \int_0^1 e^{(1-\lambda)\beta_j} f(\lambda\beta_j) d\lambda \right| \leq \left| \sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-\lambda)\beta_j} \cdot \frac{|c|^s \cdot \{m(j)\}^p}{|\beta_j| \cdot (p-1)!} d\lambda \right|$$

$$= \left| \sum_{j=1}^{r} \beta_j \cdot \frac{|c|^s \cdot \{m(j)\}^p}{|\beta_j| \cdot (p-1)!} \cdot \int_0^1 e^{(1-\lambda)\beta_j} d\lambda \right|$$

$$= \sum_{j=1}^{r} |\beta_j| \cdot \frac{|c|^s \cdot |m(j)|^p}{|\beta_j| \cdot (p-1)!} \cdot \left| \int_0^1 e^{(1-\lambda)\beta_j} dl \right|$$

$$\leq \sum_{j=1}^{r} \frac{|c|^s \cdot |m(j)|^p \cdot B}{(p-1)!},$$

όπου

$$B = \left| \max_j \int_0^1 e^{(1-\lambda)\beta_j} d\lambda \right|.$$

Αλλά για $p \to +\infty$ το $\sum\limits_{j=1}^{r} \frac{|c|^s \cdot |m(j)|^p \cdot B}{(p-1)!}$ τείνει στο 0. Άρα για $p \to +\infty$ το

πρώτο και το δεύτερο μέλος της (**) είναι άνισα. Άτοπο. Άρα το π δεν είναι αλγεβρικός.

Επομένως το π είναι υπερβατικός αριθμός.